(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 March 2002 (14.03.2002)

PCT

(10) International Publication Number
WO 02/21861 A2

(51) International Patent Classification[7]: H04Q 7/00

(21) International Application Number: PCT/IB01/01867

(22) International Filing Date:
11 September 2001 (11.09.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0022205.9 11 September 2000 (11.09.2000) GB

(71) Applicant *(for all designated States except US)*: **HONG KONG CSL LIMITED** [CN/CN]; 8/F Oxford House, Taikoo Place, 979 King's Road, Quarry Bay, Hong Kong (CN).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LEUNG, Edward, Yan, Tao** [CN/CN]; Flat 27c, Tower 1, Well On Garden, Tseung Kwan O, Hong Kong (CN). **MIDGETT, Richard** [US/CN]; c/o Hong Kong CSL Ltd, 8/F Oxford House, Taikoo Place, 979 King's Road, Quarry Bay, Hong Kong (CN). **YAU, Kwok, Wing** [CN/CN]; c/o Hong Kong CSL Ltd, 8/F Oxford House, Taikoo Place, 979 King's Road, Quarry Bay, Hong Kong (CN).

(74) Agent: **MEILMAN, Edward, A.**; Dickstein Shapiro Morin & Oshinsky LLP, 1177 Avenue of the Americas, New York, NY 10036 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 02/21861 A2

(54) Title: MOBILE COMMUNICATIONS

(57) Abstract: A method of automatically establishing a roaming service for a mobile telephone, that includes a pre-programmed SIM card, performs a Location Update in the following order. 1. Registered Public Land Mobile Network ("RPLMN"), i.e. the last registered network as stored in the SIM directory EF_{LOCI} (EF6F7E). 2. Home PLMN ("HPLMN"). 3. PLMNs contained in a "PLMN Selector" data field based on the "Operator List". 4. User - defined preferred PLMN. 5. Other PLMNs with received signal level above a predetermined strength in random order; and 6. All other PLMNs in order of descending signal strength.

MOBILE COMMUNICATIONS

The invention relates to mobile communications.

Global System for Mobile Communications ("GSM") is a technology widely adopted by mobile equipment operators throughout the world. To facilitate GSM automatic international roaming service, a set of guidelines exists so that when two GSM network operators wish to establish a roaming service, they have to establish a bilateral roaming agreement, followed by the technical and billing tests. With an automatic roaming service, mobile users do not need to change the Mobile Equipment ("ME") and the Subscriber Identity Module ("SIM"). Mobile users can make and receive calls in a visited network as if they are in a home network by using the roaming service.

Before a mobile user can use a mobile service in a visited network, the mobile user has to successfully register with the mobile service in the visited network. The procedure is called Location Update. If the home network has established a roaming service with more than one mobile operator in a same visited region, mobile users can either manually select one of the operators in the visited region, or use an auto-selection mode to perform the Location Update. According to the GSM Technical Specification 02.11, the Mobile Station ("MS")

which is comprised of ME and SIM shall perform the Location Update in the following order when the auto-selection mode is used:

1. Registered Public Land Mobile Network ("RPLMN"), i.e. the last registered network as stored in the SIM directory EF_{LOCI} (EF6F7E)

2. Home PLMN ("HPLMN")

3. PLMNs contained in the "PLMN Selector" (EF6F30) data field in the SIM (in priority order);

4. Other PLMNs with received signal level above a pre-determined value specified in the GSM specification in random order;

5. All other PLMNs in order of descending signal strength

In this order, only the "PLMN Selector" (EF6F30) will allow users to enter the preferred roaming networks. According to the GSM Technical Specification 11.11, this list is readable and can be updated by mobile users through ME.

With the introduction of Inter-Operator Tariff (IOT) by the GSM Association, network operators can negotiate with their roaming partners for a more flexible tariff. In addition, there is an increasing demand from customers for auto-selecting a better quality roaming network, and the need to prevent preferred network from

writing onto the Forbidden PLMN (FPLMN) list as a result of transient signaling fault, unsuccessful Location Update in previous registration and so on. This follows that one roaming network operator is preferred to another, based on service quality, customer services and commercial consideration. However, the existing procedure does not provide network operators with any flexibility to control the order of mobile networks in the Location Update procedure.

It is an object of the invention to enable a network operator to derive a mechanism to ensure a preferred roaming network is selected with a chosen or flexible priority.

According to a first aspect of the invention there is provided a mobile telephone arranged to automatically re-establish roaming service with a network based on an "Operator List" by modifying the Registered Public Land Mobile Network ("RPLMN") during Location Update, through the use of a pre-programmed SIM card

According to a second aspect of the invention, there is provided a method of automatically establishing a roaming service for a mobile telephone, including using a pre-programmed SIM card such that the preferred networks are selected in preference to others. Subsequently, although the Location Update is performed

in the same order as before, the networks list being accessed is modified and the mechanism is described as follows:-

1. Registered Public Land Mobile Network ("RPLMN"), i.e. the last registered network as stored in the SIM directory EF_{LOCI} (EF6F7E).
2. Home PLMN ("HPLMN");
3. PLMN contained in a "PLMN Selector" data field based on the "Operator List"
4. User-defined preferred PLMN;
5. Other PLMNs with received signal level above a pre-determined strength in random order; and

All other PLMNs in order of descending signal strength.

In an embodiment of the invention an "Operator List" with preferred roaming networks set by the home network operator is created and built into the SIM. This list can be updated by the home network operator by means of data download over the air. Examples of updating the home network operator are as follows:-

- Over the air: Normal Short Message Services ("SMS")
- Over the air: SIM Application Toolkit ("SAT") data download by SMS
- Over the air: data download by Unstructured Supplementary Service Data ("USSD")
- Over the air: SAT data download by Wireless Application Protocol ("WAP")

- Using SIM editor at services centers/shops
- Making use of Mobile Station Application Execution Environment ("MExE") platform between SIM application and Services Server application, download operator list data by the common circuit switch bearers (e.g. circuit switch 9.6kbps data) and packet switch bearers (e.g. packet switch based General Packet Radio Service ("GPRS") data)

During Location Update in auto-selection mode, MS will compare the RPLMN with the "Operator List". If the Mobile Country Code ("MCC") of the RPLMN is found in the "Operator List", the first available preferred network with the same MCC will replace that in RPLMN so that the MS searches and attempts to register to this network.

In addition, the "Operator List" will be copied to the PLMN Selector (EF6F30) and referenced by the MS during Location Update. The copying of "Operator List" over PLMN Selector (EF6F30) can be a direct copy or replaced by an indexed pre-stored list. If mobile users have entered preferred networks in PLMN Selector (EF6F30), the user-defined networks will be appended at the end, provided that there is free entry available. Thus, in auto-selection mode, the normal order of selection is unchanged, but the content of the network list is modified. As a result, the process is changed to:-

1. Registered Public Land Mobile Network

("RPLMN") with reference to "Operator List";

2. Home PLMN ("HPLMN");

3. PLMN as listed in the "Operator List" in the PLMN selector (EF6F30). The entries of the "Operator list" are stored in a specific location on the SIM e.g. EF6D30;

4. User-defined preferred PLMNs in the PLMN Selector (EF6F30). These user-defined preferred PLMNs have lower priority than those PLMNs of the "Operator List" in the PLMN Selector (EF6F30)as they are appended after the "Operator List"

5. Other PLMNs with received signal level above a pre-determined value specified in the GSM specification in random order; and

6. All other PLMNs in order of descending signal strength

Manual selection mode by the user is not affected. Mobile users can still override the auto-selection by selecting a particular network manually. A new capability can be provided to allow the home network operator flexibility to restore partly or wholly the order of Location Update procedure through data download over the air.

A roaming service for mobile operators according to the invention will now be described by way of example with reference to the accompanying drawings in which:-

Figure 1 illustrates a data structure of the "Operator List";

Figure 2 illustrates a flow at the initial power on stage;

Figure 3 illustrates an EF_{LOCI} Update Enhancement;

Figure 4 illustrates the mechanism of Over The Air ("OTA") data download; and

Figure 5 illustrates the mechanism to handle the OTA data download in a SIM card.

A new list "Operator List" is created and built in the Elementary File ("EF") in a SIM. The address of the "Operator List" is arbitrary and defined by a home operator in SIM production. In this example, the address EF6D30 is used. Figure 1 shows the data structure of this "Operator List". The size, X, of the "Operator List" can be varied. However, it must be the same as a PLMN Selector (EF6F30). According to a GSM Technical Specification, EF6F30 must contain at least 8 network entries in the format of MCC and Mobile Network Code ("MNC"). For each network entry, it will take up 3 bytes. Therefore, the minimum size of the EF6D30 is 26 bytes including the header bytes F and V. It is however

recommended to have a maximum of X less than 255 bytes since each file transfer from SIM to ME is in steps of 255 bytes for EF type. The header byte V indicates the number of valid network entries in the "Operator List". The header byte F is a flag with 4 possible values: If "F"=0, OTA update is not performed. (See Figure 4 for further explanation). Mask to Mask comparison (See Figure 2 for further explanation) between "Operator List" (EF6D30) and PLMN Selector (EF6F30) is required at power on stage. Examples of other comparison methods are as follows :

- Mask to Mask comparison between the "Operator List" (EF6D30) and the PLMN Selector (EF6F30) and the "Operator List" has higher priority than the user-defined PLMNs. The user-defined PLMNs are then appended at the end of the "Operator List" when copying onto PLMN Selector (EF6F30), provided that there is available memory spaces in the PLMN Selector (EF6F30).
- Entry to Entry comparison between the "Operator List" (EF6D30) and the PLMN Selector (EF6F30) and the "Operator List" has higher priority than the user-defined PLMNs. In this case, the redundant entries are eliminated
- Entry to Entry comparison between the "Operator List" (EF6D30) and the PLMN Selector (EF6F30). Any redundant entries are eliminated. The priorities of the entries are determined by analyzing the history of

individual roaming behaviour. This is to maximise the opportunity for ME to take an entry into usage, assuming that the mobile equipment is able to process entries in EF6F30 up to a certain limited length.

If "F"=1, OTA data download has been performed. At power on stage, when ME performs a Read binary on EF6F30, no Mask to Mask comparison between EF6D30 and EF6F30 is required. If "F"=2, only the EF_{LOCI} Update Enhancement (See Figure 3 for further explanation) is performed. If "F"=3, the enhancements mentioned in this description will be disabled and the normal order of Location Update is performed.

Figure 2 illustrates the sequence at the initial power on stage. The value F in EF6D30 is checked at the power on stage. If "F"=0, a Mask to Mask comparison between EF6D30, which has "V" valid network entries, and the first "V" entries of EF6F30 is performed. The resulting difference, i.e. network entries in EF6F30 that are not mapped in Mask to Mask comparison are identified. Afterwards, the content of "Operator List" (EF6D30) is copied onto EF6F30, followed by the difference. When searching for preferred networks, the ME is based on the new preferred networks in EF6F30 and the operator defined networks will be searched first.

Any subsequent update on the PLMN Selector (EF6F30) by

mobile users through Man Machine Interface ("MMI") is written on the EF6F30 as in a normal operation. However, the update only lasts for the session the MS is on. In the next power on, the Mask to Mask comparison is performed as described earlier. The resulting different network entries are then appended after the "Operator List" to PLMN Selector (EF6F30). Thus, the PLMN Selector (EF6F30) in ME's memory becomes the "Operator List" followed by user defined list immediately after power on. Examples of the triggering method include the following:-

- Power ON-OFF to trigger the LOCI and PLMN enhancement (the current implementation)
- 1st reading attempt on Location Information ("LOCI") after power reset on SIM triggers the LOCI enhancement
- 1st reading attempt on EF6F30 after power reset on SIM triggers the PLMN enhancement
- Any time when the SAT detects a change of MCC of RPLMN (i.e. roaming in other countries) and a subsequent re-read of EF6F30 is issued to the mobile equipment

Figure 3 illustrates the EF_{LOCI} Update Enhancement. In accordance with the GSM Technical Specification, the Registered Network (RPLMN) as listed in EF_{LOCI} is searched first in auto-selection mode. After the Mask to Mask comparison, EF_{LOCI} is checked against the Operator List (EF6D30). If the current value of EF_{LOCI} is already in

EF6D30, no modification on the EF_{LOCI} is required. Otherwise, the MCC of EF_{LOCI} is checked against that in EF6D30. If there is a match, the MNC of the first matched network in EF6D30 replaces the MNC in EF_{LOCI}. In addition, the value in EF_{BCCH} is reset. The ME is based on the modified EF_{LOCI} to search for the Registered Network (RPLMN).

Figure 4 illustrates the mechanism of OTA data download. A home network operator can update the "Operator List" by means of short message data download. The list of roaming operators in the format of MCC and MNC forms a short message content. The header bytes "NumOfEntry" and "Algorithm" indicates the number of preferred network entries and the choice of algorithm to be used. There are three possible algorithms:-

1. The operator-defined preferred roaming networks and the EF_{LOCI} update enhancement is used;
2. Only the EF_{LOCI} update enhancement is used; and
3. Neither the operator-defined preferred roaming network nor the EF_{LOCI} update enhancement is used, i.e. the original order of Location Update procedure is recovered.

In addition, due to the possible size limitation of the short message, more than 1 short message may be used in the data download. Thus, a byte is used to indicate the

session number for the data download in the short message. To avoid hacking, security measures are implemented. The Transfer Layer Protocol-Originating-Address ("TO-OA") used to send the short message must be matched with one defined in the SIM during production stage. In addition, the content of the short message, excluding the "NumOfEntry" byte and "Algorithm" byte are calculated for checksum. A simple approach is to sum the Exclusive OR ("XOR") results of two bytes pair. Other examples of possible security enhancements include:-

Content check sum plus checking of TP-OA

- Check sum algorithm based on Ki (the secret key shared between the SIM and the network) of the SIM or International Mobile Subscriber Identity ("IMSI") of the SIM

- Interactive authentication via call or supplementary services ("SS") or SMS by SAT application

Figure 5 illustrates the mechanism to handle the OTA data download in a SIM card. The short message received via OTA download triggers the resident script built in SIM card to update the flag to F=1, and the content of EF6D30 is then updated accordingly. An acknowledgement short message will be sent back to a pre-defined address. Upon the next power up, a step translation will be performed in EF6F30 to offset the user defined network list to a correct offset so that the user

defined network list is not overwritten in the case that the updated "Operator List" is longer than previous one. On the other hand, if the new "Operator List" is shorter than the previous one, the difference is removed. Then the new content of EF6D30 is copied to EF6F30 and placed before the user defined network list. The flag "F" is then reset to 0.

Embodiments enable automatic selection of the technically and quality-wise best network available for the user. The selection can also be automatically "biased" to enable the cheapest available network for each user according to users' or mobile services provider's specific commercial arrangement. A services provider is also able to remotely assist a roaming customer by up-dates transmitted to alter data in the SIM card. Normally only 8 to 16 entries are available and so a user-defined or operator defined short list of networks can be sent actively to the user depending upon the mobile telephone customers geographical habits.

Enhancements of the described roaming service can include the following:-

- Network entries which are in the operator list are removed from a Forbidden list after the triggering "after power ON/OFF"
- Operator list based on Location Update Message

received from the foreign (visited) network from our individual customers is optimised to avoid the mobile equipment limited ability in handling long PLMN selectors (EF6F30).

CLAIMS

1. A mobile telephone arranged to automatically re-establish roaming service with a network based on an "Operator List" by modifying the Registered Public Land Mobile Network ("RPLMN") during Location Update, through the use of a pre-programmed SIM card

2. A method of automatically establishing a roaming service for a mobile telephone, including using a pre-programmed SIM card such that a Location Update is performed in the following logical order:-

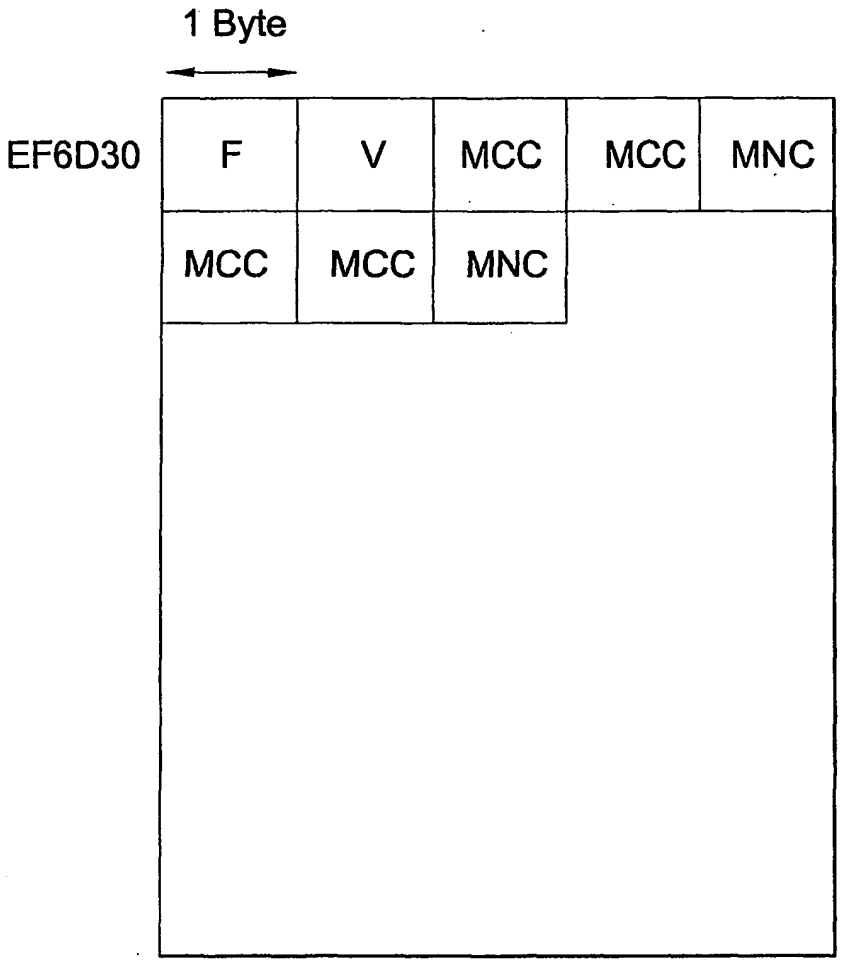
1. Registered Public Land Mobile Network ("RPLMN"), i.e. the last registered network as stored in the SIM directory EF_{LOCI} (EF6F7E)
2. Home PLMN ("HPLMN")
3. PLMNs contained in a "PLMN Selector" data field based on the "Operator List".
4. User - defined preferred PLMN
5. Other PLMNs with received signal level above a predetermined strength in random order; and
6. All other PLMNs in order of descending signal strength

3. A method according to Claim 2 in which the PLMN is stored in the "Operator List" reserved in a fixed but implementation-dependent memory location in the SIM,

e.g. EF6D30.

4. A method according to Claim 2 or 3, in which the "PLMN Selector" data comprises PLMN's listed in the "Operator List" copied on to the "PLMN Selector", the "Operator List" taking precedence over user - defined preferred PLMN's which are appended at the end of the "Operator List" in the "PLMN Selector".

5. A method according to any one of claims 2 to 4 wherein during network selection the country code of the RPLMN is compared with networks defined in the "Operator List" the most preferred network with the country code replacing the RPLMN.



File Size = X bytes
V = No of valid network entries
F = Flag

Fig. 1

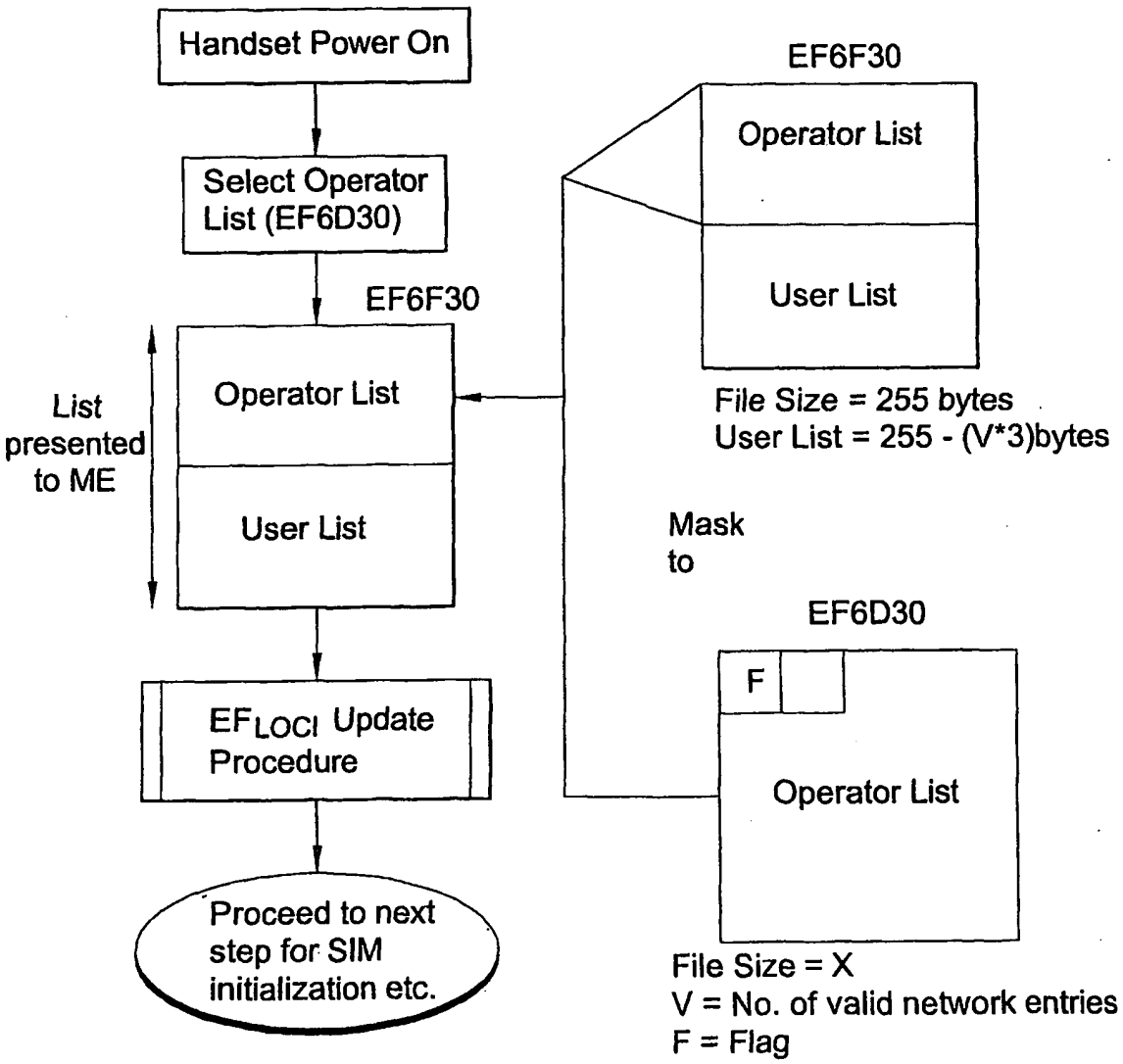

Handset Power On
Select Operator List (EF6D30)
EF6F30
Operator List
User List
List presented to ME
EF6F30
Operator List
User List
File Size = 255 bytes
User List = 255 - (V*3)bytes
Mask to
EF6D30
F
Operator List
EFLOCI Update Procedure
Proceed to next step for SIM initialization etc.
File Size = X
V = No. of valid network entries
F = Flag

Fig. 2

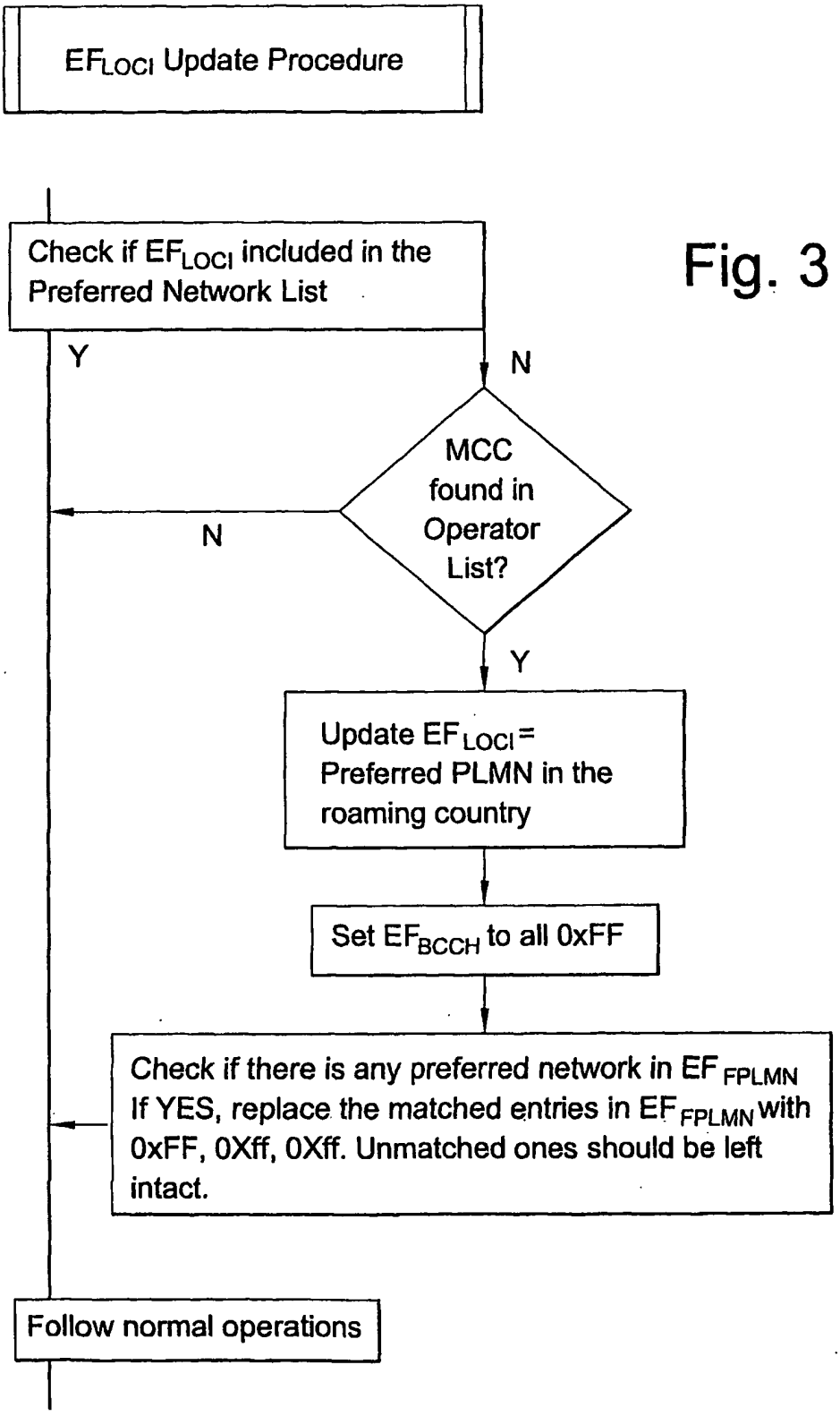

EF$_{LOCI}$ Update Procedure
Check if EF$_{LOCI}$ included in the Preferred Network List
Y
N
MCC found in Operator List?
N
Y
Update EF$_{LOCI}$ = Preferred PLMN in the roaming country
Set EF$_{BCCH}$ to all 0xFF
Check if there is any preferred network in EF$_{FPLMN}$ If YES, replace the matched entries in EF$_{FPLMN}$ with 0xFF, 0Xff, 0Xff. Unmatched ones should be left intact.
Follow normal operations

Fig. 3

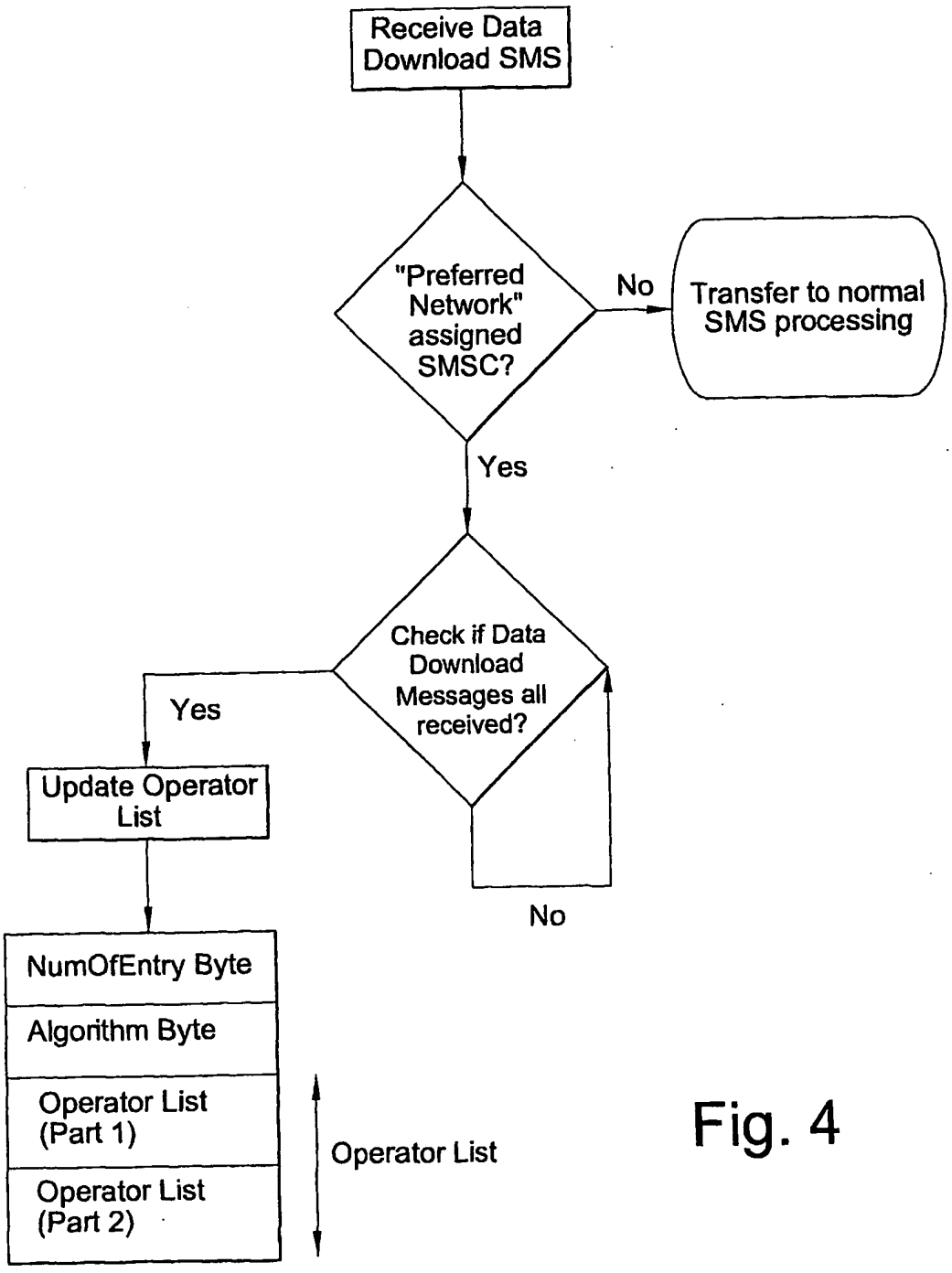
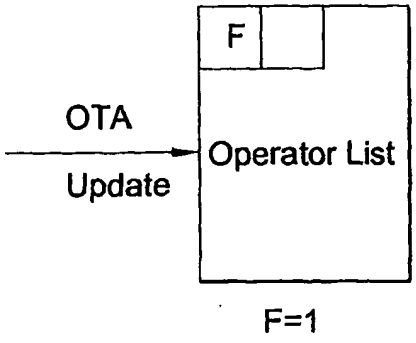

Receive Data Download SMS
"Preferred Network" assigned SMSC?
No
Transfer to normal SMS processing
Yes
Check if Data Download Messages all received?
Yes
No
Update Operator List
NumOfEntry Byte
Algorithm Byte
Operator List (Part 1)
Operator List (Part 2)
Operator List

Fig. 4


F
OTA
Update
Operator List
F=1

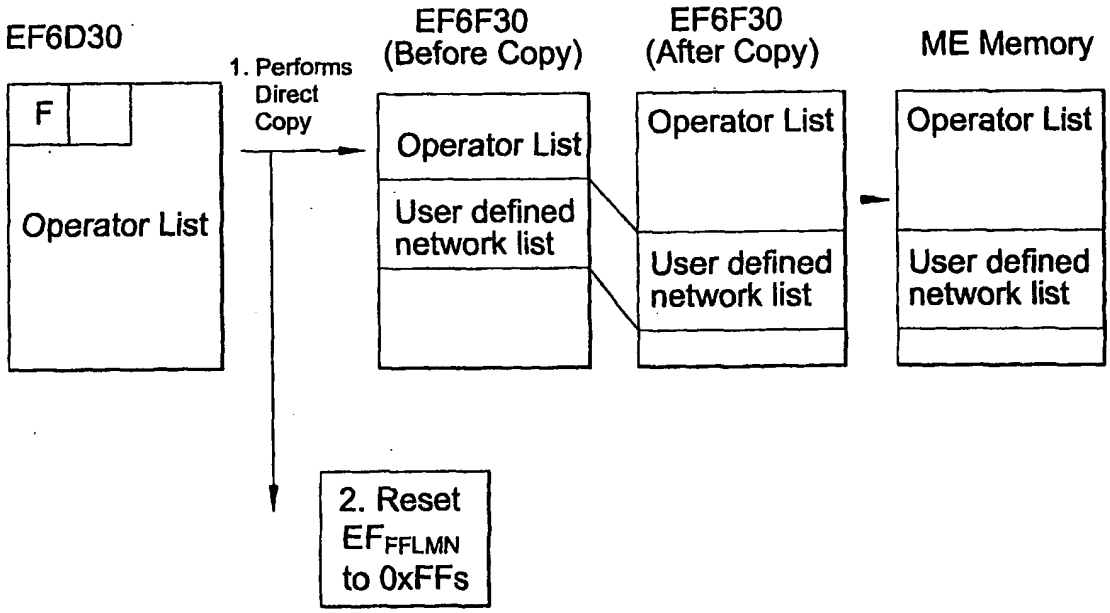

At the Next Power On after the OTA Update
EF6D30
F
Operator List
1. Performs Direct Copy
EF6F30 (Before Copy)
Operator List
User defined network list
EF6F30 (After Copy)
Operator List
User defined network list
ME Memory
Operator List
User defined network list
2. Reset EF FFLMN to 0xFFs

Fig. 5

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☑ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.